Search this guide

Table of Contents ⊕

Intro to mobile device management profiles

iOS, iPadOS, macOS and tvOS have a built-in framework that supports mobile device management (MDM). MDM lets you securely and wirelessly configure devices by sending profiles and commands to the device, whether they're owned by the user or your organisation. MDM capabilities include updating software and device settings, monitoring compliance with organisational policies, and remotely wiping or locking devices. Users can enrol their own devices in MDM, and organisation-owned devices can be enrolled in MDM automatically using Apple School Manager or Apple Business Manager. If you're using Apple Business Essentials, you can also use the device management that's built in.

There are a few concepts to understand if you're going to use MDM, so read the following sections to understand how MDM uses enrolment and configuration profiles, supervision, and payloads.

How devices enrol

Enrolment in MDM involves enrolling client certificate identities using protocols such as Automated Certificate Management Environment (ACME) or Simple Certificate Enrolment Protocol (SCEP). Devices use these protocols to create unique identity certificates for authenticating an organisation's services.

Unless enrolment is automated, users decide whether or not to enrol in MDM, and they can disassociate their devices from MDM at any time. Therefore, you want to consider incentives for users to remain managed. For example, you can require MDM enrolment for Wi-Fi network access by using MDM to automatically provide the wireless credentials. When a user leaves MDM, their device attempts to notify the MDM solution that it can no longer be managed.

For devices your organisation owns, you can use Apple School Manager, Apple Business Manager or Apple Business Essentials to automatically enrol them in MDM and supervise them wirelessly during initial setup; this enrolment process is known as *Automated Device Enrolment*.

Declarative device management

Declarative device management is an update to the existing protocol for device management that can be used in combination with the existing MDM protocol capabilities. It allows the device to asynchronously apply settings and report status back to the MDM solution without constant polling.

Status reporting allows a device to share information about its current state and if there are any changes, these can be reported to the server proactively without having to poll the device for updates. In addition to device properties, status is now reported for passcode presence and compliance, accounts and MDM app installation progress and information.

Declarations

There are four types of declarations, which are payloads that the server defines, sends to devices, and represents the policy an organisation wants to enforce on devices.

Declaration type	Description
Configurations	Configurations are similar to MDM's existing profile payloads; for example, accounts, settings and restrictions. See Declarative configurations in the MDM settings section.
Assets	Assets consist of reference data that's required by configurations for large data items and per-user data; assets have a one-to-many relationship with configurations. See Authentication credentials and identity asset settings.
Activations	Activations are a set of configurations that are applied atomically to the device and can include predicates, such as "device type is iPad" or "operating system version greater than iPadOS 16.1". There is a many-to-many relationship between activations and configurations. Activations can use an extended predicate syntax — including status items — to support complex predicate expressions. In addition, a management properties declaration allows servers to set arbitrary properties on the device, which can be directly used in activation predicates.
Management	Management is used to convey overall management state to the device, describing details about the organisation and capabilities of the MDM solution.

Status channel

The status channel is a new channel of communication where the device proactively updates the server with new information about itself. Updates of the device state are sent in a status report to the server. The server can subscribe to specific status items, so it receives only updates for the changes it cares about. Status items can also be used as expressions in activation predicates, allowing the device to operate independently, based on state changes. For more information, see Declarative status reports.

Enrolment profiles

An *enrolment profile* is one of two main ways users can enrol a personal device into an MDM solution (the other way is through an organisation's account). With this profile, which contains an MDM payload, the MDM solution sends commands and — if necessary — additional configuration profiles to the device. It can also query the device for information, such as its Activation Lock status, battery level and name.

When a user removes an enrolment profile, all configuration profiles, their settings and Managed Apps based on that enrolment profile are removed with it. There can be only one enrolment profile on a device at a time.

After the enrolment profile is approved, either by the device or the user, *configuration profiles* containing payloads are delivered to the device. You can then wirelessly distribute, manage and configure apps and books purchased through Apple School Manager, Apple Business Manager or Apple Business Essentials. Users can install apps or apps can be installed automatically, depending on the type of app it is, how it's assigned and whether the device is *supervised*. For more information, see About Apple device supervision.

Configuration profiles

A *configuration profile* is an XML file (ending in .mobileconfig) consisting of payloads that load settings and authorisation information onto Apple devices. Configuration profiles automate the configuration of settings, accounts, restrictions and credentials. These files can be created by an MDM solution or Apple Configurator, or they can be created manually.

Because configuration profiles can be encrypted and signed, you can restrict their use to a specific Apple device and — with the exception of usernames and passwords — prevent anyone from changing the settings. You can also mark a configuration profile as being locked to the device.

If your MDM solution supports it, you can distribute configuration profiles as a mail attachment, via a link on your own web page or through the MDM solution's built-in user portal. When users open the mail attachment or download the configuration profile using a web browser, they're prompted to begin configuration profile installation.

For more information about profile installation and Lockdown Mode, see the Apple Support article About Lockdown Mode.

Note: You can use Apple Configurator for Mac to add configuration profiles (automatically or manually) to iOS, iPadOS and Apple TV devices. For more information, see the Apple Configurator User Guide for Mac.

As an administrator, you can deliver a configuration profile that can change settings for an entire device or for a single user:

- *Device profiles* can be sent to devices and device groups, and apply device settings to the entire device.

  iPhone, iPad and Apple TV have no way to recognise more than one user, so configuration profiles created from iOS, iPadOS and tvOS payloads and settings are always device profiles. Although iPadOS profiles are device profiles, iPad devices configured for Shared iPad can support profiles based on the device or the user.

- *User profiles* can be sent to users and user groups, and apply user settings to just the respective users.

  Mac computers can have multiple users, so payloads and settings for macOS profiles can be based on the device or the user.

Device and user settings vary according to where they reside: Settings installed at the system level reside in a device channel. Settings installed for a user reside in a user channel.

Profile removal

How you remove profiles depends on how they were installed. The following sequence indicates how a profile can be removed:

1. All profiles can be removed by wiping the device of all data.

2. If the device was enrolled in MDM using Apple School Manager, Apple Business Manager or Apple Business Essentials, the administrator can choose whether the *enrolment* profile can be removed by the user or whether it can be removed only by the MDM server itself.

3. If the profile is installed by an MDM solution, it can be removed by that specific MDM solution or by the user unenrolling from MDM by removing the enrolment configuration profile.

4. If the profile is installed on a supervised device using Apple Configurator, that supervising instance of Apple Configurator can remove the profile.

5. If the profile is installed on a supervised device manually or using Apple Configurator and the profile has a removal password payload, the user must enter the removal password to remove the profile.

6. All other profiles can be removed by the user.

An account installed by a configuration profile can be removed by removing the profile. A Microsoft Exchange ActiveSync account, including one installed using a configuration profile, can be removed by the Microsoft Exchange Server by issuing the account-only remote wipe command.

Important: If users know the device passcode, they can remove manually installed configuration profiles from iPhone and iPad that aren't supervised, even if the option is set to "never". Users on macOS can do the same thing only if the user knows an administrator's username and password. They can do this using the `profiles` command-line tool, System Settings (in macOS 13 or later) or System Preferences (in macOS 12.0.1 or earlier). In macOS 10.15 or later, as with iOS and iPadOS, profiles installed with MDM must be removed with MDM or they are removed automatically upon unenrolment from MDM.

Supported Apple devices

The following Apple devices have a built-in framework that supports MDM:

- iPhone with iOS 4 or later
- iPad with iOS 4.3 or later or iPadOS 13.1 or later
- Mac computers with OS X 10.7 or later
- Apple TV with tvOS 9 or later

Note: Not all options are available in all MDM solutions. To learn which MDM options are available for your devices, consult your MDM vendor's documentation.

Published Date: 24 October 2022

See also

Deploy devices using Apple School Manager, Apple Business Manager or Apple Business Essentials

Choose an MDM solution

Apple at Work website

Apple and Education

Helpful? Yes No

Previous
What's new

Next
Intro to MDM payloads